ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

How Europe’s General Data Protection Regulation Rewrote Global Data Protection Rules

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***Individual rights.*** Under GDPR, individuals have the “right to access” and “to be forgotten.”
- ***Personal data has changed.*** No longer name, photo, and address, “personal data” now covers IP addresses, geolocation, and biometric data.
- ***Penalties.*** Penalties under GDPR are mandatory and uniform across all EU states.
- ***Privacy by design.*** GDPR requires that the privacy of data collected be accounted for at every step of the process — especially the beginning.

> *“I am tired of clicking the ‘I accept’ pop-up every time I open Google Chrome. Whether I need to do a financial transaction or shop for new clothing, or even post pictures on social media like Instagram or Facebook, it’s always there. What is this new regulation? Why are all our customers demanding an amendment to our existing contract? What is this new regulation all about? What are the penalties for breaching it? As a service provider, what is our liability and obligation toward our customers? Can you enlighten me and other sales folks on this matter?”*

This quote is from a member of Infosys’ sales team when we were discussing the General Data Protection Regulation (GDPR) and how it will impact one of our largest financial customers in Germany.

I replied, “Well, that is a great point, and I can definitely explain GDPR and its impact so far.”

This article will discuss how to educate your sales team members by explaining (1) why everyone is so concerned about data; (2) recent cases; (3) how GDPR differs from previous data laws; (4) jurisdictional scope of GDPR and liability of third-party organizations; (5) when and against whom claims can be made under GDPR; (6) and what’s to come.

What’s happening now?

The frantic requests to opt-in to receive future messages happened because companies were scrambling to comply with GDPR, which went into effect on May 25, 2018, and supersedes the Data Protection Directive (DPD). The primary aim of the legislation is to give individuals control of their data. The law applies to all enterprises within the European Economic Area (EU countries plus Iceland, Liechtenstein, and Norway) and companies that process the data of EU subjects, regardless of location.

GDPR initially made headlines because of its eye-popping fines. There are two levels of fines. The first tier prescribes a fine of €10 million or a maximum of double the total worldwide annual turnover of the preceding financial year, whichever is higher.

The second tier prescribes a fine of €20 million or up to four percent of the total worldwide annual turnover of the preceding financial year for not complying with an order from a supervisory authority

(this could mean US$9.3 billion for Google and Facebook combined).[1]

The maximum prescribed punishment isn't necessarily handed out in each case. Various factors such as nature, gravity, and duration of the infringement, and whether it was intentional or negligent, are factors. As are technical and organizational measures implemented by the organization, the types of personal data involved, the actions taken to mitigate the damage suffered by individuals, any previous infringements by the organization or data processor, the degree of cooperation with the regulator, the way the regulator found out about the infringement, the manner in which the infringement became known to the supervisory authority, in particular, whether and to what extent the organization notified the infringement, and whether, and to what extent, the controller or processor notified the infringement are taken into consideration while deciding the quantum of penalty in each case.

While no fines have been leveled yet, there are several cases ongoing under GDPR right now. ICANN vs. EPAG Domain Services GmbH is considered to be one of the first rulings. In this case, the practical application of the regulations as well as principles relating to the processing of personal data was called for interpretation by a German court.

One of the first cases of extraterritorial jurisdiction being applied was by the UK watchdog, Information Commissioner Office, against AggregateIQ, an analytics company based in Canada. The notice sent to the company was also the first UK GDPR notice. According to Cambridge Analytica (CA) whistleblower Chris Wylie, AIQ used algorithms from Facebook data held by CA to build software to target Republican voters in the 2016 US election. Under the terms of the notice, AggregateIQ is required to cease processing any personal data of EU citizens for the purposes of data analytics, political campaigning, or any other advertising purposes within 30 days of the date of the notice. AggregateIQ may appeal against this notice especially on the extraterritorial jurisdiction of Information Commissioner Office.

Within hours of GDPR coming into force, privacy group noyb.eu, led by activist Max Schrems, filed complaints against four companies, namely Facebook, Google, Instagram, and WhatsApp, alleging that the companies are in breach of GDPR because they have adopted a *"take it or leave it approach."* Customers must agree to having their data collected, shared, and used for targeted advertising, or delete their accounts. The privacy group contends this forces people to accept wide-ranging data collection in exchange for using a service — which is prohibited under GDPR.

Another case is the leak by British Airways of sensitive passenger information between August 5 and September 21, 2018. While the breach was reported within the mandated 72 hours, significant safety norms and errors that could have been fixed were not followed. There are class action suits filed against British Airways, for non-material damage as laid out under GDPR. However, the fine has not been imposed yet. Some think that the airline can be hit by a huge fine amounting to hundreds of millions of dollars. If the airline's parent group, International Airlines Group (IAG), is held accountable instead, the number may climb even higher.

UK customers of Ticketmaster have been warned they could be at risk of fraud or identity theft after the global ticketing group revealed a major data breach that has affected tens of thousands of people. The customers who bought concert, theater, and sporting event tickets between February and June 2018 may have been affected by the incident, which involved malicious software being used to steal people's names, addresses, email addresses, phone numbers, payment details, and Ticketmaster login details. The Ticketmaster data breach had affected up to 40,000 people who bought tickets between September 2017 and June 23, 2018. However, no fine has been levied yet.

Key words and associated meanings

- ***Data controller:*** a natural/legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.
- ***Data processor:*** a natural/legal person, public authority, agency, or other body that processes personal data on behalf of the controller.
- ***Supervising authority:*** the Independent public authority that is established by a Member State pursuant to article 51 of GDRP.
- ***Data processing:*** any operation(s) that is/are performed on personal data or sets of personal data, by automated means or not (such as collection, recording, organization, storage, etc.).

The key duties of data processors (which are also applicable to third parties)[1]

- A processor cannot engage another processor without specific authorization of the controller.
- Processing activities governed by a contract that expressly sets out the nature and type of processing, types of data, categories of data subjects, stipulates that processor will act only on the controller's instructions and all security measures will be complied with while processing.
- If the processor feels that the controller's instructions infringe on GDPR, then the processor must notify the controller.
- When the data processor employs another processor, the same obligations of the former will apply to the second processor. If the second processor breaches any obligations, full liability will be imposed on the initial processor.
- If a processor does the job of a controller and decides on the means and purpose of processing, then the processor will be deemed to be the controller.

GDPR rewrites the rules of the Data Protection Directive

While the DPD, which was created in 1995, had good intentions and worked well for when it was established, a lot has changed in the world of information and technology since then. The European Union decided that the time had come for the law to change to keep pace with the fast-changing ecosystem of information and technology. Key changes were introduced in the following areas:

Redefining personal data

Where personal data was previously defined as a person's name, photo, email address, phone number, address, or any personal identification number (social security, bank account, etc.), under GDPR it has a much broader definition. Things like IP addresses, mobile device identifiers, geolocation, and biometric data (fingerprints, retina scans, etc.) will also constitute personal data. In addition, things like an individual's physical, psychological, genetic, mental, economic, cultural, and social identity are also covered by GDPR.

The expansive definition of personal data is significant because it reflects the changes in technology

and the way organizations are now required to collect, store, and use personal data. At one end, GDPR has provided greater control to data subjects by giving them the right to be informed about what data is collected, for what reason, and how it is used. Specific consent by data subjects is required either through a web form, including a link to the privacy statement, or in an email.

On the other end, it has complicated the marketing and sales efforts for companies. GDPR has restricted and narrowed the way the data is collected, processed, and stored by such companies. This means that a company cannot assume that they have permission to send mass email campaigns just because they have the emails of data subjects. Sales pitches on autopilot mode have to be stopped immediately.

Information governance and security individual rights

GDPR requires compliance at the inception of the business concept. This is called “privacy by design.” The privacy of the data collected is accounted for at every step of the process, and most importantly at the beginning of a project. Privacy by design also requires that controllers discard personal data when it is no longer required.

Impact assessments should be conducted to ensure the security of the personal data collected and processed. These impact assessments are required for automated data processing activities, large scale processing of certain kinds of data, and systematic monitoring of a publicly accessible area on a large scale, which means an area where personal data can be publicly accessible like social media platforms.

Data breach notification and penalties

The GDPR’s simple requirement rule requires that data controllers notify the supervisory authority of a personal data breach within 72 hours of learning about it. This notification should lay out the nature of the breach, the categories, and an approximate number of individuals impacted, and the contact information of the organization’s data protection officer. The notification should also include the likely consequences of the breach, and what the controller has done to address and mitigate the breach. A data processor is required to notify a controller of the data breach “without undue delay.” When a data breach occurs, controllers must notify individuals “when the personal data breach is likely to result in a high risk to the rights and freedoms of individuals” and they must do so “without undue delay.” This notification should also include the contact information of the organization’s data protection officer, the likely outcomes of the breach, and how the company plans on rectifying the situation.

Under the DPD, the number of administrative penalties was left up to the discretion of the member states. It was seen that the fines imposed by the member states on the defaulters were very small and were rarely applied. This deterrent mechanism has been made stronger under GDPR. Penalties under GDPR are *mandatory* and *uniform* across all EU states. These penalties can be imposed for any negligent or intentional violation of GDPR.

Individual rights

GDPR puts great emphasis on the rights of individuals. An explicit opt-in consent will be required for the processing of any personal data. Consent for the use of personal data has to be informed, specific, and unambiguous. The goal is to stop the long, drawn-out user agreements that are often overlooked. Descriptions for data use should be short and straight to the point. Consumers cannot be

asked to agree to contract terms in exchange for their consent. Companies are required to review their terms of use agreements. In addition, different types of data require separate consent to avoid the idea of an “all or nothing” choice to individuals. Silence or inactivity also does not constitute consent — the consumer needs to affirmatively provide consent.

Under GDPR, data subjects have the “right of access,” which is the right to obtain from the data controller information on how their data is being used (where and for what purpose). The controller must provide this information along with a copy of their personal data, free of charge, electronically. This empowers data subjects and promotes transparency.

Just as individuals are empowered with the right to access their personal data, they are also provided with the right to “be forgotten” and, if asked by any data subject, the controller must erase all of their personal data, cease further use of that data, and, if applicable, halt any third party’s use of that data.

Data controllers vs. data processors

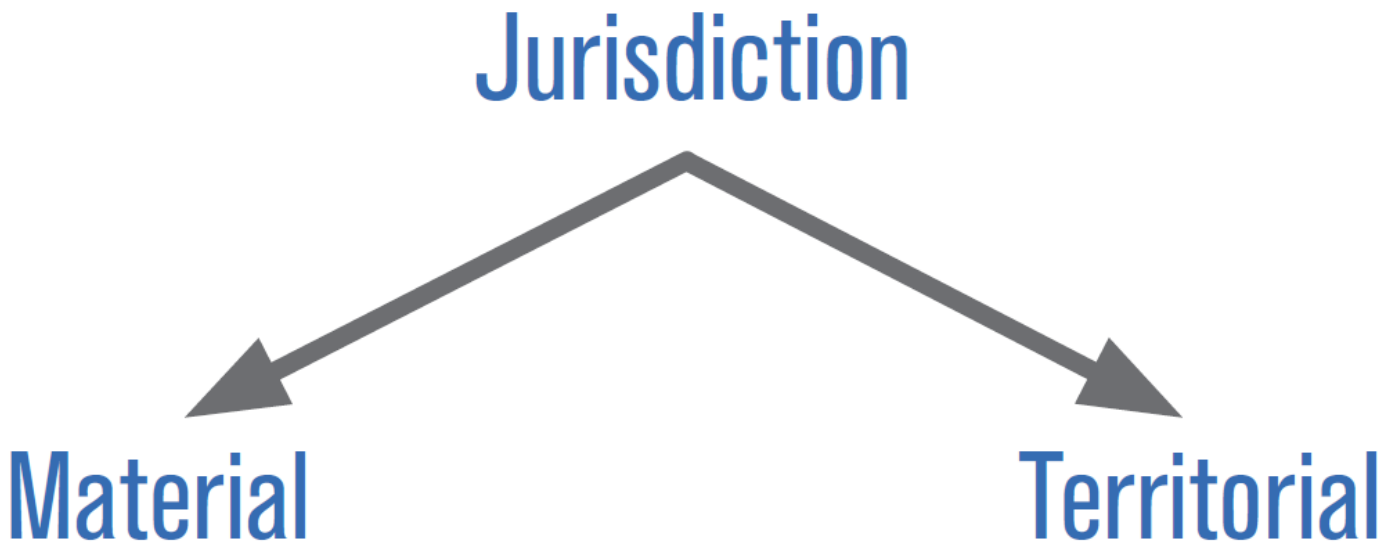
A significant difference between the DPD and GDPR is the accountability of data processors. Data processors are defined as “the natural legal person, public authority, agency or other body, which processes data on behalf of the controller.” Under the DPD, only data controllers[2] were held accountable for any breach. GDPR requires that a data protection officer must be appointed when the core activities of the controller or processor involve “regular and systematic monitoring of data subjects on a large scale.” This officer can be an established employee within your company. The officer is required to be knowledgeable about how the company is collecting or processing[3] personal data. Both controllers and processors are required to maintain documentation describing their data protection policies and keep a record of their data processing activities. The only exception applies to organizations with fewer than 250 employees. In that case, they do not have to maintain records of processing, whether they are a controller or a processor.

2 Data Controller is defined as “Natural/legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.”

3 Processing means “any operation(s) which is performed on personal data or sets of personal data, by automated means or not, (such as collection, recording, organization, storage etc.).”

Jurisdictional scope of GDPR

There are two major categories of GDPR jurisdictional scope: material and territorial scope.



Material scope[4] includes the processing of personal data, wholly or partly, where the personal data forms, or is intended to form, part of a filing system. The following activities fall outside material scope: (1) activity that falls outside the scope of Union law such as activities related to national security; (2) activities conducted by Member States when carrying out activities in relation to the common foreign and security policy of the European Union; (3) activities by a natural person in the course of a purely personal or household activity; and (4) activities by competent authorities for purposes of prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, such as the location of a terrorist cell.

Territorial scope[5] extends to (1) processing of personal data by a controller or a processor established in the European Union, regardless of whether the processing takes place in the EU region or not. For example, take a company based in Germany that processes data outside the European Union. The determining factor is whether the controller or processor has an establishment in the EU/EEA. The term establishment is not defined in GDPR. However, an establishment implies the effective and real exercise of activity through stable arrangements, as confirmed by the CJEU's Weltimmo decision.

4 Article 2 of the GDPR Regulation.

5 Article 3 of the GDPR Regulation.

It also extends to (2) processing of personal data of data subjects who are in the European Union by a controller or processor not established in the European Union, where the processing activities may include: (a) offering of goods/services, irrespective of whether payment is required; and (b) monitoring of behavior if it happens in the European Union. For example, an online ecommerce company based in India provides web access to data subjects in the EU region. It offers goods/products in the EU region in Euro currency, using German language to connect with data subjects in the European Union. In this case, factors such as the use of a language or a currency generally used in one or more member states with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the EU/EEA, may make it apparent that the controller envisages offering goods or services to data subjects in the EU/EEA.[6]

And (3) processing of personal data by a controller not established in the European Union, but in a

place where Member State law applies by virtue of public international law, such as companies like Infosys or TCS that are established outside the European Union but process the personal data of EU data subjects by providing information technology services to clients in the European Union.

Liability of third-party organization

The GDPR definition of a third party is a natural/legal person, public authority, agency or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data. Note that a third party can include a processor that has been hired by another processor to carry out data processing operations. A data processor is a party that processes data on behalf of the controller and is hired by the controller.

When can claims can be made under GDPR?

Every data subject — more than half a billion people in the European Union — has the right to lodge a complaint with the supervising authority if there's reason to think GDPR was violated. The supervising authority must inform the complainant on the progress and outcome of his complaint. In the event that the supervising authority does not inform the complainant on any progress within three months of filing the complaint, the complainant will have the right of judicial remedy against that supervisory authority.[7]

Any data subject who has suffered material or non-material damage will have the right to receive compensation from the controller or processor. A controller is generally liable for any damage. On the other hand, a processor is liable when (1) the processor has not complied with regulations specifically meant for processors and when (2) the processor has acted contrary to the lawful instructions of the controller. When a controller and processor are involved in the same processing violation then they will be held entirely liable for the damage caused to the data subject.[8]

There are no uniform fines laid down under GDPR for data breach cases. Each case is required to be judged based on the circumstances and a set of factors laid under GDPR.[9] Member states have the power to prescribe rules for proportionate penalties for infringements not mentioned within GDPR.[10]

7 Article 78 of the GDPR.

8 Article 82 of the GDPR.

9 Article 83 of the GDPR.

10 Article 84 of the GDPR.

What's to come?

GDPR is gaining momentum and ensuring that organizations raise their security standards in terms of protecting and handling personal data of data subjects across the world. The supervisory authority under GDPR is not levying penalties on companies on a prima facie basis but is using detailed due diligence, investigations, and warnings to companies.

GDPR is making the right impact and serving the purpose for which it was implemented. It is ensuring that the rights of data subjects are well protected and that the companies handling such data are taking sufficient measures to avoid breaches or leaks of personal data. GDPR is striving for the right balance of public interest protection interest and economic growth.

With all the above information, I hope you can educate your sale folks on why there are so many pop-ups asking for consent — and the risks and goals of GDPR.

Vijita Verma

Senior Corporate Counsel

Infosys Ltd

Vijita Verma is senior corporate counsel at Infosys Ltd. She has more than 12 years of experience in commercial contracts and has worked with clients across the globe.